ABSTRACT

A data encryption method performed with ring arithmetic operations using a residue number multiplication process wherein a first conversion to a first basis is done using a mixed radix system and a second conversion to a second basis is done using a mixed radix system. In some embodiments, a modulus C is be chosen of the form $2^w - L$, wherein C is a w-bit number and L is a low Hamming weight odd integer less than $2^{(w-1)/2}$. And in some of those embodiments, the residue mod C is calculated via several steps. P is split into 2 w-bit words H_1 and L_1. S_1 is calculated as equal to $L_1 + (H_1 2^{x1}) + (H_1 2^{x2}) + \ldots + (H_1 2^{xk}) + H_1$. S_1 is split into two w-bit words H_2 and L_2. S_2 is computed as being equal to $L_2 + (H_2 2^{x1}) + (H_2 2^{x2}) + \ldots + (H_2 2^{xk}) + H_2$. S_3 is computed as being equal to $S_2 + (2^{x1} + \ldots + 2^{xk} + 1)$. And the residue is determined by comparing S_3 to 2^w. If $S_3 < 2^w$, then the residue equals S_2. If $S_3 \geq 2^w$, then the residue equals $S_3 - 2^w$.